National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

Hanfodion Seibr: Gofynion ar gyfer Seilwaith TG v3.3

Mae'r wybodaeth hon wedi'i heithrio o dan Ddeddf Rhyddid Gwybodaeth 2000 (FOIA) a gall fod wedi'i heithrio o dan ddeddfwriaeth gwybodaeth arall y DU. Cyfeiriwch unrhyw ymholiadau FOIA at ncscinfoleg@ncsc.gov.uk.
Mae'r holl ddeunydd yn Hawlfraint y Goron yn y DU. Ebrill 2026

Cyber Essentials: Gofynion ar gyfer Seilwaith TG f3.3

Cynnwys

Beth sy'n newydd yn y fersiwn hon 3
A. Cyflwyno'r rheolaethau technegol 3
B. Diffiniadau 4
C. Creu copi wrth gefn o'ch data 5
D. Cwmpas 6
Trosolwg o gwmpas Cyber Essentials 6
Rheoli asedau a Cyber Essentials 7
(i) Dod â'ch dyfais eich hun (BYOD) 8
(ii) Gweithio gartref ac o bell 9
(iii) Dyfeisiau di-wifr 9
(iv) Gwasanaethau cwmwl 9
(v) Cyfrifon a ddefnyddir gan drydydd partïon a seilwaith a reolir 11
(vi) Dyfeisiau a ddefnyddir gan drydydd partïon 11
(vii) Datblygu meddalwedd 12
E. Gofynion yn ôl thema rheolaeth dechnegol 13
1. Waliau tân 13
Nod 13
Cyflwyniad 13
Gofynion 14
2. Ffurfweddiad Diogel 15
Nod 15
Cyflwyniad 15
Gofynion 15
3. Rheoli Diweddariadau Diogelwch 17
Nod 17

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Cyflwyniad 17
Gofynion 17
4. Rheoli Mynediad Defnyddwyr 18
Nod 18
Cyflwyniad 19
Gofynion 20
Dilysu heb gyfrinair 20
Dull dilysu aml-ffactor 21
Dilysu drwy gyfrinair 22
5. Amddiffyn rhag maleiswedd 23
Nod 23
Cyflwyniad 24
Gofynion 24
F. Canllawiau pellach 25
Dim ymddiriedaeth a Cyber Essentials 25

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Beth sy'n newydd yn y fersiwn hon

- Rhoddir diffiniad o ‘wasanaethau cwmwl’
- Diffiniad wedi'i ddiweddaru o Dilysu Heb Gyfrinair i gynnwys FIDO2
- Datganiad diffiniol bod yn rhaid cynnwys gwasanaethau cwmwl o fewn y cwmpas
- Cod Ymarfer ar gyfer Diogelwch Meddalwedd wedi'i gyflwyno yn yr adran Datblygu Meddalwedd
- Nid yw meini prawf y cwmpas yn cyfeirio at 'gysylltiadau annibynadwy' mwyach
- Pwysleisir pwysigrwydd creu copïau wrth gefn o ddata

A. Cyflwyno'r rheolaethau technegol

Rydym wedi trefnu'r gofynion o dan bum rheolaeth dechnegol:

1. Waliau tân
2. Ffurfweddiad Diogel
3. Rheoli Diweddariadau Diogelwch
4. Rheoli Mynediad Defnyddwyr
5. Amddiffyn rhag maleiswedd

Fel sefydliad sy'n gwneud cais am ardystiad o dan gynllun Cyber Essentials, eich cyfrifoldeb chi yw sicrhau bod eich sefydliad yn bodloni'r holl ofynion. Mae'n bosibl hefyd y bydd angen i chi ddarparu tystiolaeth cyn y gall eich corff ardystio roi tystysgrif i chi ar y lefel rydych yn gwneud cais amdani.

Beth y dylech ei wneud gyntaf:

- Pennu **ffin y cwmpas** ar gyfer eich sefydliad, ac yna bennu beth yw'r cwmpas o fewn y ffin hon.
- Adolygu pob un o'r **pum thema rheolaeth dechnegol** a'r **rheolaethau y maent yn eu corffori fel gofynion**.
- Cymryd y camau angenrheidiol i **sicrhau bod eich sefydliad yn bodloni pob gofyniad** sydd ei angen arno ar gyfer y cwmpas a bennwyd gennych.

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

B. Diffiniadau

Mae **ymgeisydd** yn cyfeirio at y sefydliad sy'n ceisio ardystiad, neu weithiau'r unigolyn sy'n gweithredu fel y prif bwynt cyswllt, yn dibynnu ar y cyd-destun
Ystyr **gwasanaeth cwmwl** yw gwasanaeth ar-alw a all dyfu, a gaiff ei letya ar seilwaith a rennir ac y ceir mynediad ato drwy'r rhyngrwyd. At ddibenion Cyber Essentials, ceir mynediad at wasanaeth cwmwl drwy gyfrif (a all fod yn fanylion a ddyroddwyd gan eich sefydliad neu'n gyfeiriad e-bost a ddefnyddir at ddibenion busnes) a bydd yn storio neu'n prosesu data ar gyfer eich sefydliad
Rhwydwaith preifat rhithwir yw **VPN corfforaethol** sy'n cysylltu yn ôl i leoliad eich swyddfa, neu i wal dân rithwir neu ar y cwmwl. Mae'n rhaid i chi weinyddu'r VPN fel y gallwch gymhwyso rheolaethau'r wal dân
Mae **dyfeisiau** yn cynnwys pob math o letywyr, cyfarpar rhwydweithio, gweinyddion, rhwydweithiau, a dyfeisiau defnyddiwr terfynol, megis cyfrifiaduron bwrdd gwaith, gliniaduron, cleientiaid tenau, llechi a ffonau clyfar — boed yn ffisegol neu'n rhithwir
Meddalwedd y mae gennych hawl gyfreithiol i'w defnyddio yw **meddalwedd drwyddedig a gefnogir** ac y mae gwerthwr wedi ymrwymo i'w chefnogi drwy ddarparu ffyrdd o atgyweirio gwendidau yn rheolaidd. Mae'n rhaid i'r gwerthwr ddarparu dyddiad yn y dyfodol pan na fydd yn darparu'r rhain mwyach. (Noder nad oes rhaid i'r gwerthwr fod wedi creu'r feddalwedd yn y lle cyntaf, ond rhaid iddo allu addasu'r feddalwedd wreiddiol er mwyn creu ffyrdd o atgyweirio gwendidau)
Mae **Dilysu Aml-ffactor** yn ddull o ddilysu defnyddiwr sy'n defnyddio dau ffactor dilysu neu fwy
Mae **data sefydliadol** yn cynnwys unrhyw ddata electronig sy'n perthyn i'ch sefydliad, er enghraifft, negeseuon e-bost, dogfennau, data cronfa ddata, data ariannol

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Mae **gwasanaeth sefydliadol** yn cynnwys unrhyw gymwysiadau meddalwedd, cymwysiadau cwmwl, gwasanaethau cwmwl, byrddau gwaith rhyngweithiol defnyddwyr a datrysiadau rheoli dyfeisiau symudol y mae eich sefydliad yn berchen arnynt neu'n tanysgrifio iddynt. Er enghraifft: cymwysiadau ar y we, Microsoft 365, Google Workspace, cynwysyddion rheoli dyfeisiau symudol, Citrix Desktop, datrysiadau Virtual Desktop neu deleffoni IP
Mae **dilysu heb gyfrinair** yn ddull o gadarnhau pwy yw'r defnyddiwr sy'n defnyddio ffactor heblaw gwybodaeth. Mae enghreifftiau yn cynnwys y canlynol ond nid ydynt yn gyfyngedig iddynt: dilyswyr FIDO2, data biometrig, allweddi neu docynnau diogelwch, codau untro, codau QR a hysbysiadau gwthio.
Ystyr **cwmpas**yw'r rhwydweithiau, yr asedau caledwedd a meddalwedd, a'r gwasanaethau cwmwl sydd wedi'u cynnwys yn yr asesiad
Dyfeisiau yw **gweinyddion** sy'n darparu data sefydliadol neu wasanaethau i ddyfeisiau eraill fel rhan o fusnes eich sefydliad
Mae **meddalwedd** yn cynnwys systemau gweithredu, cymwysiadau masnachol parod, estyniadau, dehonglwyr, sgriptiau, llyfrgelloedd, meddalwedd rhwydwaith a wal dân a chadarnwedd llwybrydd
Mae **is-set** yn rhan o'r sefydliad y mae ei rwydwaith wedi'i wahanu oddi wrth weddill y sefydliad gan wal dân neu rwydwaith ardal leol rithwir (VLAN)
Mae **ffyrdd o atgyweirio gwendidau** yn cynnwys patsys, diweddariadau, atgyweiriadau cofrestrfa, newidiadau ffurfweddu, sgriptiau neu unrhyw ddull arall a ragnodir gan y gwerthwr i atgyweirio gwendid hysbys

C. Creu copi wrth gefn o'ch data

Nid yw creu copi wrth gefn o'ch data yn un o ofynion technegol Cyber Essentials. Fodd bynnag, rydym yn argymell yn gryf eich bod yn defnyddio proses briodol i gadw copïau wrth gefn o'ch gwybodaeth.
Mae creu copi wrth gefn o'ch gwybodaeth yn golygu creu'r copi a'i gadw ar ddyfais arall neu ar y cwmwl (ar-lein).

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Mae creu copi wrth gefn yn rheolaidd yn golygu y bydd fersiwn ddiweddar o'ch gwybodaeth wedi'i chadw bob amser. Bydd hyn yn eich helpu i adfer yn gynt os bydd eich data'n mynd ar goll neu'n cael eu dwyn.

Os oes systemau ar gael ar gyfer creu copïau wrth gefn o ddata yn awtomatig, dylech ystyried eu troi ymlaen. Bydd hyn yn cadw eich gwybodaeth ar y cwmwl yn rheolaidd, heb i chi orfod cofio.

Os byddwch yn cadw copi wrth gefn o'ch gwybodaeth ar gof bach USB neu yriant caled allanol, cofiwch ei ddatgysylltu o'ch cyfrifiadur pan na fydd y broses gadw yn mynd rhagddi.

D. Cwmpas

Trosolwg o gwmpas Cyber Essentials

Dylai eich asesiad a'ch ardystiad gwmpasu'r seilwaith TG cyfan a ddefnyddir i gyflawni busnes eich sefydliad neu, os oes angen, is-set a reolir ar wahân ac wedi'i diffinio'n dda. Y naill ffordd neu'r llall, mae'n rhaid i chi ddiffinio ffin y cwmpas yn glir, sef: yr uned fusnes sy'n ei reoli, ffin y rhwydwaith a'r lleoliad ffisegol. Rhaid i chi gytuno ar y cwmpas â'r corff ardystio cyn dechrau'r asesiad.

Gellir defnyddio is-set i ddiffinio beth sydd **yn y cwmpas** a'r tu allan i'r cwmpas ar gyfer eich ardystiad Cyber Essentials.

Noder: Sefydliadau sy'n dewis cwmpas sy'n cynnwys eu seilwaith TG cyfan sy'n cyflawni'r amddiffyniad gorau ac yn sicrhau hyder eu cwsmeriaid.

Lle mae rhannau o seilwaith sefydliad wedi'u heithrio o'r cwmpas, bydd angen i chi gyfiawnhau'r rheswm dros gwmpas rhannol i'ch asesydd.

Mae'r gofynion yn berthnasol i bob dyfais a meddalwedd yn y cwmpas ac sy'n bodloni unrhyw un o'r amodau hyn:

- gallu derbyn cysylltiadau â'r rhwydwaith sy'n dod i mewn o ddyfeisiau sydd wedi cysylltu â'r rhyngrwyd
- gallu sefydlu cysylltiadau allan â dyfeisiau drwy'r rhyngrwyd

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

- rheoli llif data rhwng unrhyw un o'r dyfeisiau uchod a'r rhyngrwyd

Nid yw cwmpas nad yw'n cynnwys dyfeisiau defnyddwyr terfynol yn dderbyniol.

Os caiff data neu wasanaethau eich sefydliad eu lletya ar wasanaethau cwmwl, rhaid i'r gwasanaethau hyn fod o fewn y cwmpas. Rhaid cynnwys gwasanaethau cwmwl o fewn y cwmpas

Rheoli asedau a Cyber Essentials

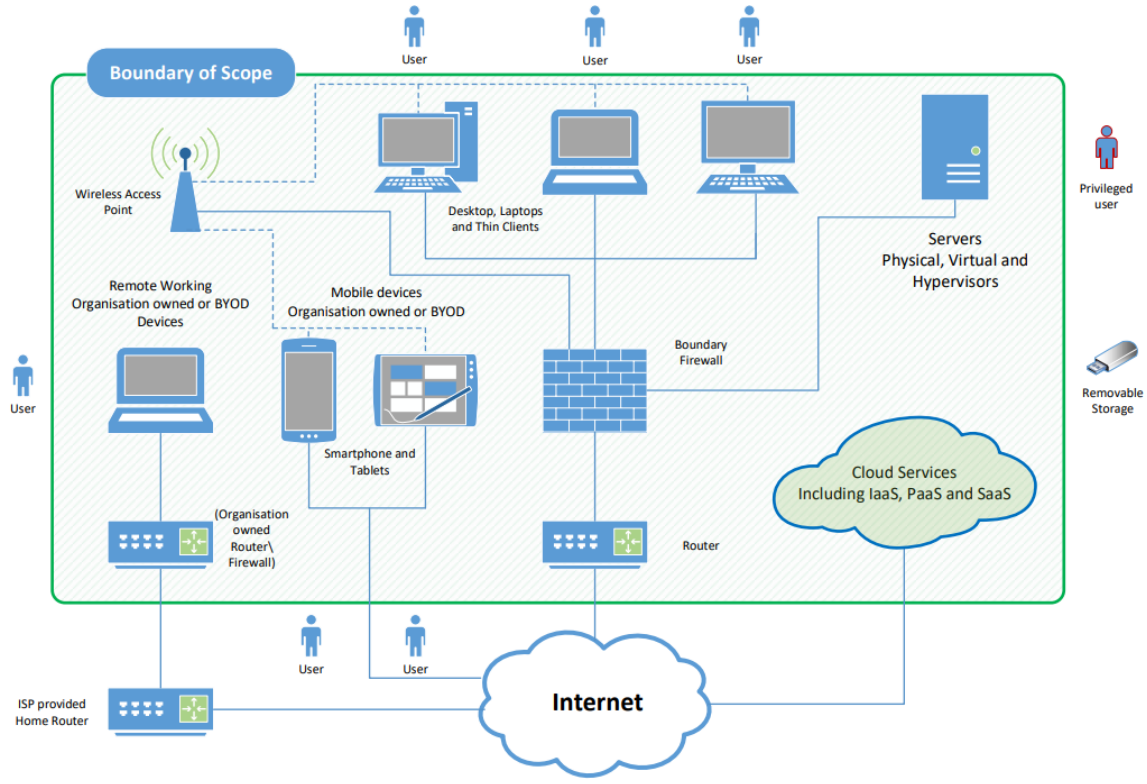
Nid yw rheoli asedau yn un o reolaethau penodol Cyber Essentials, ond gall rheoli asedau yn effeithiol helpu i fodloni'r pum rheolaeth, felly dylid ei ystyried fel swyddogaeth diogelwch craidd.

Mae'r rhan fwyaf o weithrediadau busnes yn dibynnu ar ryw agwedd ar reoli asedau, ac ni ddylid ystyried seiberddiogelwch ar ei ben ei hun, neu fel prif ddefnyddiwr gwybodaeth asedau. Mae'r swyddogaethau hyn yn cynnwys gweithrediadau TG, cyfrifyddu ariannol, trwyddedau rheoli meddalwedd, caffael a logisteg. Mae'n bosibl na fydd angen yr un wybodaeth ar bob un, ond bydd y gofynion perthnasol yn gorgyffwrdd ac yn rhannu dibyniaethau. Bydd integreiddio a chydgysylltu prosesau rheoli asedau ar draws eich sefydliad yn helpu i leihau neu reoli unrhyw achosion o wrthdaro rhwng y swyddogaethau hyn.

Nid yw rheoli asedau yn effeithiol yn golygu creu rhestrau neu gronfeydd data na chânt eu defnyddio fyth. Mae'n golygu creu, sefydlu a chynnal gwybodaeth awdurdodol a chywir am eich asedau sy'n galluogi gweithrediadau o ddydd i ddydd a phrosesau gwneud penderfynu effeithlon pan fydd eu hangen arnoch. Yn benodol, bydd yn eich helpu i olrhain a rheoli dyfeisiau wrth iddynt gael eu cyflwyno i'ch busnes.

Mae gan y Ganolfan Seiberddiogelwch Genedlaethol ganllawiau cynhwysfawr i sefydliadau ar reoli asedau.

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©



Ffigur 1: Cwmpas y gofynion ar gyfer seilwaith TG

(i) Dod â'ch dyfais eich hun (BYOD)

Yn ogystal â dyfeisiau symudol neu ddyfeisiau o bell y mae'r sefydliad yn berchen arnynt, mae dyfeisiau y mae defnyddwyr yn berchen arnynt sy'n cael mynediad at ddata neu wasanaethau'r sefydliad (fel y'u diffinnir uchod) hefyd **yn rhan o'r cwmpas**. Fodd bynnag, mae'r holl ddyfeisiau symudol neu ddyfeisiau o bell a ddefnyddir at y dibenion canlynol **yn unig**:

- cymwysiadau llais brodorol
- cymwysiadau testun brodorol
- mae cymwysiadau dilysu aml-ffactor **y tu allan i'r cwmpas**.

Yn draddodiadol, roedd dyfeisiau defnyddwyr yn cael eu rheoli'n fewnol, a oedd yn sicrhau cysondeb ym mhob rhan o'r sefydliad. Mae ardystio rheolaethau diogelwch yn y ffordd hon yn symlach gan fod gwneuthuriad safonol y gellir cyfeirio ato.

Mae BYOD yn cymhlethu pethau, gan fod defnyddwyr yn cael mwy o ryddid i ‘addasu’ eu profiad sy'n golygu bod rhoi'r rheolaethau ar waith mewn ffordd gyson yn fwy heriol. Dylai defnyddio'r diffiniadau o ran data a

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

gwasanaethau sefydliadol i orfodi polisïau mynediad cryf ddileu rhywfaint o'r amwysedd hwn.

I gael rhagor o wybodaeth a chyngor ar ddefnyddio BYOD, gweler canllawiau'r Ganolfan Seiberddiogelwch Genedlaethol.

(ii) Gweithio gartref ac o bell

Ein dull gweithredu diofyn yw bod pob dyfais gweithio gartref/o bell gorfforaethol neu BYOD a ddefnyddir ar gyfer busnes eich sefydliad o fewn cwmpas Cyber Essentials.

Os bydd eich sefydliad yn rhoi llwybrydd i'r sawl sy'n gweithio gartref/o bell, bydd y llwybrydd hwnnw'n rhan o'r cwmpas hefyd.

Bydd pob llwybrydd arall **y tu allan i'r cwmpas** sy'n golygu y bydd angen i chi roi rheolaethau wal dân Cyber Essentials (megis wal dân meddalwedd) ar ddyfeisiau defnyddwyr.

Os bydd y sawl sy'n gweithio gartref/o bell yn defnyddio VPN corfforaethol, bydd ei ffin rhyngrwyd ar wal dân y cwmni neu wal dân rithwir/ar y cwmwl.

(iii) Dyfeisiau di-wifr

Mae dyfeisiau di-wifr (gan gynnwys pwyntiau mynediad di-wifr):

- **o fewn y cwmpas** os gallant gyfathrebu â dyfeisiau eraill drwy'r rhyngrwyd
- **y tu allan i'r cwmpas** os nad yw'n bosibl i ymosodwr ymosod yn uniongyrchol drwy'r rhyngrwyd (nid yw cynllun Cyber Essentials yn ymwneud ag ymosodiadau y gellir ond eu lansio o fewn ystod signal y ddyfais ddi-wifr)
- **y tu allan i'r cwmpas** os ydynt yn rhan o lwybrydd ISP yn y cartref neu'r lleoliad pell

(iv) Gwasanaethau cwmwl

Os caiff data neu wasanaethau eich sefydliad eu lletya ar wasanaethau cwmwl, rhaid i'r gwasanaethau hyn fod **o fewn y cwmpas**.

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Ar gyfer gwasanaethau cwmwl, **y sefydliad sy'n gwneud cais sydd bob amser yn gyfrifol** am sicrhau y caiff pob rheolaeth ei rhoi ar waith, ond gall rhai o'r rheolaethau gael eu rhoi ar waith gan ddarparwr y gwasanaeth cwmwl. Mae pwy sy'n rhoi pa reolaeth ar waith yn dibynnu ar y math o wasanaeth cwmwl. Rydym yn ystyried tri math gwahanol o wasanaeth cwmwl:

- **Seilwaith fel Gwasanaeth (IaaS)** – bydd darparwr y cwmwl yn darparu gweinyddion rhithwir a chyfarpar rhwydwaith a gaiff eu ffurfweddu a'u rheoli gan eich sefydliad, yn debyg i gyfarpar ffisegol. Mae enghreifftiau o IaaS yn cynnwys Rackspace, Google Compute Engine, neu Amazon EC2
- **Llwyfan fel Gwasanaeth (PaaS)** - bydd darparwr y cwmwl yn darparu ac yn rheoli'r seilwaith sylfaenol, a bydd eich sefydliad yn darparu ac yn rheoli'r cymwysiadau. Mae enghreifftiau o PaaS yn cynnwys Azure Web Apps ac Amazon Web Services Lambda
- **Meddalwedd fel Gwasanaeth (SaaS)** – bydd darparwr y cwmwl yn darparu cymwysiadau, a bydd eich sefydliad yn ffurfweddu'r gwasanaethau wedyn. Mae'n rhaid i chi sicrhau bod y gwasanaeth yn cael ei ffurfweddu yn ddiogel. Mae enghreifftiau o SaaS yn cynnwys Microsoft 365, Dropbox a Gmail

Bydd pwy sy'n rhoi'r rheolaethau ar waith yn amrywio, yn dibynnu ar sut y mae'r gwasanaeth cwmwl wedi'i ddylunio. Mae'r tabl isod yn esbonio pwy y gellid disgwyl iddo roi pob rheolaeth ar waith fel arfer:

Gofyniad	**IaaS**	**PaaS**	**SaaS**
Waliau tân	Eich sefydliad a darparwr y cwmwl	Darparwr y cwmwl a'ch sefydliad hefyd weithiau	Darparwr y cwmwl
Ffurfweddiad Diogel	Eich sefydliad a darparwr y cwmwl	Eich sefydliad a darparwr y cwmwl	Eich sefydliad a darparwr y cwmwl
Rheoli Diweddariadau Diogelwch	Eich sefydliad a darparwr y cwmwl	Eich sefydliad a darparwr y cwmwl	Darparwr y cwmwl

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Rheoli Mynediad Defnyddwyr	Eich sefydliad	Eich sefydliad	Eich sefydliad
Amddiffyn rhag Maleiswedd	Eich sefydliad a darparwr y cwmwl	Darparwr y cwmwl a'ch sefydliad hefyd weithiau	Darparwr y cwmwl

Tabl 1: Esboniad o bwy all roi pob rheolaeth ar waith fel arfer

Mewn achosion pan fydd darparwr y cwmwl yn rhoi un o'r rheolaethau ar waith ar eich rhan, mae'n rhaid i chi sicrhau bod darparwr y cwmwl wedi ymrwymo i roi hyn ar waith drwy gymalau contractiol neu ddogfennau y cyfeirir atynt yn y contract, megis datganiadau diogelwch neu ddatganiadau preifatrwydd. Bydd darparwyr cwmwl yn aml yn esbonio sut maent yn rhoi mesurau diogelwch ar waith mewn dogfennau a gyhoeddir yn eu canolfannau ymddiriedaeth, gan gyfeirio at 'fodel cyfrifoldeb a rennir'.

(v) Cyfrifon a ddefnyddir gan drydydd partïon a seilwaith a reolir

Mae pob cyfrif y mae eich sefydliad yn berchen arno o fewn y cwmpas, hyd yn oed pan gaiff y cyfrifon hynny eu defnyddio gan drydydd parti, megis cyflenwr, contractwr neu Ddarparwr Gwasanaeth a Reolir (MSP) er mwyn rheoli neu gefnogi eich seilwaith.

Os ydych yn defnyddio gwasanaethau a reolir yn allanol (megis gwasanaeth gweinyddu o bell), rhaid i chi allu cadarnhau bod rheolaethau technegol Cyber Essentials yn cael eu bodloni a dylech allu dangos hyn yn eich atebion i'r asesiad.

(vi) Dyfeisiau a ddefnyddir gan drydydd partïon

Rhaid i bob dyfais defnyddiwr terfynol y mae eich sefydliad yn berchen arni sy'n cael ei rhoi ar fenthyg i drydydd parti gael ei chynnwys yng nghwmpas yr asesiad.

Ar gyfer dyfeisiau nad yw eich sefydliad yn berchen arnynt, mae'r tabl isod yn esbonio beth sy'n rhan o'r cwmpas a beth sydd y tu allan iddo:

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Rôl	Dyfeisiau y mae eich sefydliad yn berchen arnynt	Dyfeisiau y mae trydydd parti yn berchen arnynt	BYOD
Cyflogai	✓	**Dd/G**	✓
Gwirfoddolwr	✓	**Dd/G**	✓
Ymddiriedolwr	✓	**Dd/G**	✓
Cynorthwyydd ymchwil mewn prifysgol	✓	**Dd/G**	✓
Myfyriwr	✓	**Dd/G**	✗
Gweinyddwr MSP	✓	✗	✗
Contractwr trydydd parti	✓	✗	✗
Cwsmer	✓	✗	✗

Tabl 2: Beth sy'n rhan o'r cwmpas a beth sydd y tu allan iddo ar gyfer dyfeisiau nad yw eich sefydliad yn berchen arnynt

Allwedd: ✓ O fewn y cwmpas ✗ Y tu allan i'r cwmpas

Ar gyfer dyfeisiau y tu allan i gwmpas yr asesiad, bydd eich sefydliad yn gyfrifol o hyd am gadarnhau bod dyfeisiau sy'n rhyngweithio â gwasanaethau a data sefydliadol wedi'u ffurfweddu'n gywir. Mater i chi yw penderfynu sut i gyflawni hyn, gan ei fod y tu allan i gwmpas yr asesiad.

(vii) Datblygu meddalwedd

Mae cymwysiadau masnachol ar y we sydd ar gael i'r cyhoedd (yn hytrach nag apiau a ddatblygir yn fewnol) yn rhan o'r cwmpas yn ddiofyn. Mae elfennau pwrpasol ac wedi'u haddasu o gymwysiadau ar y we y tu allan i'r cwmpas. Y ffordd orau o liniaru gwendidau mewn cymwysiadau yw prosesau datblygu a phrofi cadarn yn unol ag arferion gorau masnachol.

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Gweler y Cod Ymarfer ar gyfer Diogelwch Meddalwedd am ragor o fanylion.

E. Gofynion yn ôl thema rheolaeth dechnegol

1. Waliau tân

Yn gymwys i: waliau tân ffiniol, cyfrifiaduron bwrdd gwaith, gliniaduron, llwybryddion, gweinyddion, IaaS, PaaS, SaaS

Nod

Gwneud yn siŵr mai dim ond gwasanaethau rhwydwaith diogel ac angenrheidiol y gellir cael gafael arnynt drwy'r rhyngrwyd.

Cyflwyniad

Mae pob dyfais yn rhedeg gwasanaethau rhwydwaith i'w galluogi i gyfathrebu â dyfeisiau a gwasanaethau eraill. Drwy gyfyngu ar fynediad at y gwasanaethau hyn, byddwch yn llai agored i ymosodiadau. Gallwch wneud hyn drwy ddefnyddio waliau tân neu ddyfeisiau rhwydwaith sydd â swyddogaeth wal dân. Ar gyfer gwasanaethau cwmwl, gallwch gyflawni hyn drwy ddefnyddio polisïau llif data.

Dyfais rhwydwaith yw wal dân ffiniol a all gyfyngu ar draffig rhwydwaith sy'n dod i mewn ac yn mynd allan o wasanaethau ar ei rwydwaith o gyfrifiaduron a dyfeisiau symudol. Gall helpu i amddiffyn rhag ymosodiadau seiber drwy roi cyfyngiadau ar waith, a elwir yn 'rheolau wal dân', a all ganiatáu neu rwystro traffig yn dibynnu ar ei ffynhonnell, ei gyrchfan a'r math o brotocol cyfathrebu.

Fel arall, os nad yw eich sefydliad yn rheoli'r rhwydwaith y mae dyfais yn cysylltu ag ef, rhaid i chi ffurfweddu wal dân meddalwedd ar y ddyfais. Mae hon yn gweithio yn yr un ffordd â wal dân ffiniol ond bydd ond yn amddiffyn yr un ddyfais y mae wedi'i ffurfweddu arni. Mae'r dull gweithredu hwn yn caniatáu rheolau mwy penodol ac yn golygu bod y rheolau yn berthnasol

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

i'r ddyfais lle bynnag y caiff ei defnyddio. Ond dylech nodi bod hyn yn creu gorbenion gweinyddol mwy wrth reoli rheolau wal dân.

Gofynion

Mae'n rhaid i chi amddiffyn pob dyfais o fewn y cwmpas gyda wal dân wedi'i ffurfweddu'n gywir (neu swyddogaeth wal dân ar gyfer dyfais rhwydwaith).

Gwybodaeth: Mae wal dân meddalwedd wedi'i rhagosod ar systemau gweithredu'r rhan fwyaf o gyfrifiaduron bwrdd gwaith a gliniaduron bellach. Cynghorwn fod hon yn cael ei throi ymlaen yn hytrach na chymhwysiad wal dân trydydd parti.

Ar gyfer pob wal dân (neu ddyfeisiau rhwydwaith â swyddogaeth wal dân), rhaid i'ch sefydliad wneud y canlynol:

- newid cyfrineiriau gweinyddol diofyn i gyfrinair cryf ac unigryw (gweler dilysu drwy gyfrinair) – neu analluogi mynediad gweinyddol o bell yn llwyr
- atal mynediad at y rhyngwyneb gweinyddol (a ddefnyddir i reoli ffurfweddiad y wal dân) o'r rhyngwyd, oni bai fod angen busnes clir ac wedi'i ddogfennu, a bod y rhyngwyneb wedi'i amddiffyn gan un o'r rheolaethau canlynol:
    - dull dilysu aml-ffactor (gweler y manylion isod)
    - rhestr caniatáu IP sy'n cyfyngu mynediad i ystod fach o gyfeiriadau dibynadwy ynghyd â dull dilysu drwy gyfrinair a reolir yn briodol
- rhwystro cysylltiadau heb eu dilysu sy'n dod i mewn yn ddiofyn
- sicrhau bod rheolau wal dân sy'n dod i mewn yn cael eu cymeradwyo a'u dogfennu gan berson awdurdodedig, a chynnwys yr angen busnes yn y ddogfennaeth
- dileu neu analluogi rheolau wal dân diangen, pan na fydd eu hangen mwyach

Gwneud yn siŵr eich bod yn defnyddio wal dân meddalwedd ar ddyfeisiau a ddefnyddir ar rwydweithiau annibynadwy, megis llecynnau Wi-Fi cyhoeddus.

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

2. Ffurfweddiad Diogel

Yn gymwys i: gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, cleientiaid tenau, IaaS, PaaS, SaaS

Nod

Sicrhau bod cyfrifiaduron a dyfeisiau rhwydwaith wedi'u ffurfweddu'n briodol er mwyn:

- lleihau gwendidau
- darparu'r gwasanaethau sy'n ofynnol i gyflawni eu rôl yn unig

Cyflwyniad

Nid yw ffurfweddiadau diofyn cyfrifiaduron a dyfeisiau rhwydwaith yn ddiogel bob amser. Bydd ffurfweddiadau safonol 'yn syth allan o'r bocs' yn aml yn cynnwys un man gwan neu fwy, megis:

- cyfrif gweinyddol sydd â chyfrinair diofyn wedi'i ragosod ac sy'n hysbys yn gyhoeddus, neu nad oes dull dilysu aml-ffactor wedi'i alluogi ar ei gyfer
- cyfrifon defnyddwyr sydd wedi'u rhag-alluogi ond sy'n ddiangen (weithiau gyda breintiau mynediad arbennig)
- cymwysiadau neu wasanaethau sydd wedi'u rhagosod ond sy'n ddiangen

Gall y gosodiadau diofyn hyn ganiatáu ymosodwyr i gael mynediad at wybodaeth sensitif eich sefydliad heb awdurdod.

Ond drwy ddefnyddio rhai rheolaethau technegol syml wrth osod cyfrifiaduron a dyfeisiau rhwydwaith, gallwch leihau gwendidau ac amddiffyn yn erbyn mathau cyffredin o ymosodiadau.

Gofynion

Cyfrifiaduron a dyfeisiau rhwydwaith

Mae'n rhaid i'ch sefydliad reoli eich cyfrifiaduron a'ch dyfeisiau rhwydwaith yn rhagweithiol. Mae'n rhaid i chi wneud y canlynol yn rheolaidd:

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

- dileu ac analluogi cyfrifon defnyddwyr diangen (megis cyfrifon gwesteion a chyfrifon gweinyddol na chânt eu defnyddio)
- newid unrhyw gyfrineiriau diofyn neu gyfrineiriau y gellir eu dyfalu ar gyfrifon (gweler dilysu drwy gyfrinair)
- dileu neu analluogi meddalwedd ddiangen (gan gynnwys cymwysiadau, cyfleustodau system a gwasanaethau rhwydwaith)
- analluogi unrhyw nodwedd sy'n rhedeg yn awtomatig sy'n caniatáu gweithredu ffeil heb awdurdodiad gan y defnyddiwr (er enghraifft, pan gaiff ei lawrlwytho)
- sicrhau bod defnyddwyr wedi'u dilysu cyn caniatáu iddynt gael mynediad at ddata neu wasanaethau sefydliadol
- sicrhau bod rheolaethau priodol ar gyfer cloi'r ddyfais (gweler 'datgloi dyfeisiau' isod) ar gyfer defnyddwyr sy'n bresennol yn gorfforol

Manylion ar gyfer datgloi dyfeisiau

Os bydd angen presenoldeb corfforol defnyddiwr er mwyn cael mynediad at wasanaethau dyfais (megis mewngofnodi i liniadur neu ddatgloi ffôn symudol), rhaid i fanylion megis cyfrinair, PIN neu system fiometrig fod ar waith cyn y gall defnyddiwr gael mynediad at y gwasanaethau

Rhaid i chi ddiogelu eich dewis ddull dilysu (a all fod yn ddilysiad biometrig, drwy gyfrinair neu gyda PIN) rhag ymosodiadau grymus. Os bydd modd ffurfweddu, dylech ddefnyddio un o'r dulliau canlynol:

- cyfyngu ar nifer yr ymgeisiau, fel bod yr amser y mae'n rhaid i'r defnyddiwr aros rhwng ymgeisiau yn cynyddu gyda phob ymgais aflwyddiannus. Ni ddylech ganiatáu mwy na 10 cynnig mewn 5 munud
- cloi dyfeisiau ar ôl dim mwy na 10 ymgais aflwyddiannus

Os na fydd y gwerthwr yn caniatáu i chi ffurfweddu'r uchod, defnyddiwch osodiad diofyn y gwerthwr.

Rhaid defnyddio rheolaethau technolegol i reoli ansawdd manylion. Os mai dim ond i ddatgloi dyfais mae manylion, defnyddiwch gyfrinair neu PIN sydd o leiaf 6 nod o hyd. Pan gaiff y manylion i ddatgloi'r ddyfais eu defnyddio ar gyfer dilysu hefyd, rhaid i chi ddefnyddio'r gofynion cyfrinair llawn a ddisgrifir yn Rheolaethau Mynediad Defnyddwyr.

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

3. Rheoli Diweddariadau Diogelwch

Yn gymwys i: gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, waliau tân, llwybryddion, IaaS, PaaS, SaaS

Nod

Sicrhau nad yw dyfeisiau a meddalwedd yn agored i broblemau diogelwch hysbys pan fo ffyrdd o'u hunioni ar gael.

Cyflwyniad

Gall unrhyw ddyfais sy'n rhedeg meddalwedd gynnwys diffygion diogelwch, a elwir yn wendidau.

Deuir o hyd i wendidau mewn pob math o feddalwedd yn rheolaidd. Unwaith y deuir o hyd iddynt, bydd unigolion neu grwpiau maleisus yn symud yn gyflym i gamddefnyddio (neu 'gamfanteisio ar') wendidau er mwyn ymosod ar gyfrifiaduron a rhwydweithiau.

Mae gwerthwyr cynhyrchion yn darparu ffyrdd o atgyweirio gwendidau a nodir mewn cynhyrchion y maent yn dal i'w cefnogi, ar ffurf patsys, diweddariadau diogelwch, atgyweiriadau cofrestrfa, sgriptiau, newidiadau ffurfweddu neu unrhyw ddull arall a ragnodir gan y gwerthwr i atgyweirio gwendid hysbys. Mae'n bosibl y darperir y rhain i gwsmeriaid yn syth neu'n unol ag amserlen ryddhau reolaidd (bob mis efallai).

Gofynion

Mae'n rhaid i chi sicrhau bod yr holl feddalwedd o fewn y cwmpas yn gyfredol. Mae'n rhaid i bob meddalwedd ar ddyfeisiau sydd o fewn y cwmpas:

- fod wedi'i thrwyddedu a'i chefnogi
- cael ei dileu oddi ar ddyfeisiau pan na fydd yn cael ei chefnogi mwyach neu pan gaiff ei dileu o'r cwmpas gan ddefnyddio is-set ddiffiniedig sy'n atal yr holl draffig i'r rhyngrwyd neu ohono
- bod â diweddariadau wedi'u galluogi lle bo'n bosibl
- cael ei diweddaru, gan gynnwys ffyrdd o atgyweirio gwendidau, o fewn 14 diwrnod* i gael ei rhyddhau:

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

- pan fo'r diweddariad yn atgyweirio gwendidau a ddisgrifir gan y gwerthwr fel ‘critigol’ neu ‘risg uchel’
- pan fo'r diweddariad yn ymdrin â gwendidau â sgôr sylfaen CVSS v3 o 7 neu fwy
- nid oes unrhyw fanylion am lefel y gwendidau y mae'r diweddariad a ddarperir gan y gwerthwr yn eu hatgyweirio

Noder: Er mwyn bod mor ddiogel â phosibl, argymhellwn yn gryf (ond nid yw'n orfodol) fod yr holl ddiweddariadau a ryddhawyd yn cael eu rhoi ar waith o fewn 14 diwrnod i'w rhyddhau.

*****Mae'n bwysig bod diweddariadau yn cael eu rhoi ar waith cyn gynted â phosibl. Ystyrir bod 14 diwrnod yn gyfnod rhesymol i allu cyflawni'r gofyniad hwn. Byddai cyfnod hwy yn gyfystyr â risg ddiogelwch ddifrifol ac mae'n bosibl na fyddai cyfnod byrrach yn ymarferol.

Gwybodaeth: Os bydd y gwerthwr yn defnyddio termau gwahanol i ddisgrifio difrifoldeb gwendidau, gweler y diffiniad manwl gywir yn y System Sgorio Gwendidau Cyffredin (CVSS). At ddiben cynllun Cyber Essentials, gwendidau ‘critigol’ neu ‘risg uchel’ yw'r rheini sydd â sgôr sylfaen CVSS v3 o 7 neu uwch neu rai a nodir gan y gwerthwr fel ‘critigol’ neu ‘risg uchel'.

Rhybudd: Bydd rhai gwerthwyr yn rhyddhau diweddariadau diogelwch ar gyfer sawl mater sy'n amrywio o ran difrifoldeb fel un diweddariad. Os bydd unrhyw ddiweddariad o'r fath yn cwmpasu materion ‘critigol’ neu ‘risg uchel’ yna rhaid ei osod o fewn 14 diwrnod.

4. Rheoli Mynediad Defnyddwyr

Yn gymwys i: gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, IaaS, PaaS, SaaS

Nod

Sicrhau bod cyfrifon defnyddwyr:

- yn cael eu neilltuo i unigolion awdurdodedig yn unig

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

- ond yn rhoi mynediad at y cymwysiadau, y cyfrifiaduron a'r rhwydweithiau hynny sydd eu hangen ar y defnyddiwr i gyflawni ei rôl

Cyflwyniad

Mae pob cyfrif defnyddiwr gweithredol yn eich sefydliad yn hwyluso mynediad at ddyfeisiau a chymwysiadau, ac at wybodaeth fusnes sensitif. Drwy wneud yn siŵr mai dim ond unigolion awdurdodedig sydd â chyfrifon defnyddwyr, a'u bod ond yn cael cymaint o fynediad ag sydd ei angen arnynt i gyflawni eu rôl, byddwch yn lleihau'r risg y caiff gwybodaeth ei dwyn neu ei dinistrio.

O gymharu â chyfrifon defnyddwyr arferol, mae gan gyfrifon â breintiau mynediad arbennig fynediad uwch at ddyfeisiau, cymwysiadau a gwybodaeth. Os bydd y cyfrifon hyn dan fygythiad, gallai ymosodwr fanteisio ar eu mynediad uwch er mwyn llygru gwybodaeth ar raddfa fawr, tarfu ar brosesau busnes neu gael mynediad heb awdurdod at ddyfeisiau eraill yn y sefydliad.

Mae gan gyfrifon gweinyddol freintiau arbennig o uchel, er enghraifft. Fel arfer, bydd y cyfrifon hyn yn caniatáu i'r defnyddiwr wneud y canlynol:

- gweithredu meddalwedd a all wneud newidiadau sylweddol a newidiadau sy'n gysylltiedig â diogelwch i'r system weithredu
- gwneud newidiadau i'r system weithredu ar gyfer rhai defnyddwyr neu bob un
- creu cyfrifon newydd a dyrannu breintiau

Bydd gan bob math o weinyddwyr y math hwn o gyfrif, gan gynnwys gweinyddwyr parth a gweinyddwyr lleol.

Mae hyn yn bwysig oherwydd os bydd defnyddiwr yn agor URL neu atodiad e-bost maleisus, fel arfer byddai'r faleiswedd yn cael ei gweithredu â'r un lefel braint â chyfrif y defnyddiwr. Dyma pam mae'n bwysig bod yn arbennig o ofalus wrth ddyrannu a defnyddio cyfrifon â breintiau.

Enghraifft: Mae Jody wedi mewngofnodi â chyfrif gweinyddol. Os bydd Jody yn agor URL neu atodiad e-bost maleisus, mae'n debygol y byddai unrhyw faleiswedd gysylltiedig yn cael breintiau gweinyddol. Yn anffodus, dyma'n union beth sy'n digwydd. Gan ddefnyddio breintiau gweinyddol

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Jody, mae math o faleiswedd a elwir yn feddalwedd wystlo yn amgryptio'r holl ddata ar y rhwydwaith ac yna'n mynnu pridwerth. Llwyddodd y feddalwedd wystlo i amgryptio llawer mwy o ddata nag y byddai wedi bod yn bosibl gyda breintiau defnyddiwr safonol, sy'n golygu bod y broblem yn llawer mwy difrifol.

Gofynion

Mae'n rhaid i'ch sefydliad reoli eich cyfrifon defnyddwyr a'r breintiau mynediad sy'n caniatáu mynediad at eich data a'ch gwasanaethau sefydliadol. Mae'n bwysig nodi bod hyn hefyd yn cynnwys cyfrifon trydydd parti – er enghraifft, cyfrifon a ddefnyddir gan eich gwasanaethau cymorth. Hefyd, mae angen i chi ddeall sut mae cyfrifon defnyddwyr yn dilysu ac yn rheoli'r dull dilysu yn briodol.

Mae hyn yn golygu bod yn rhaid i'ch sefydliad wneud y canlynol:

- sicrhau bod proses ar waith i greu a chymeradwyo cyfrifon defnyddwyr
- dilysu defnyddwyr gan ddefnyddio manylion unigryw cyn rhoi mynediad at gymwysiadau neu ddyfeisiau
- dileu neu analluogi cyfrifon defnyddwyr pan na fydd eu hangen mwyach (er enghraifft, pan fydd defnyddiwr yn gadael y sefydliad neu ar ôl cyfnod diffiniedig o anweithgarwch ar y cyfrif)
- rhoi dull dilysu aml-ffactor ar waith, pan fo ar gael – rhaid i brosesau dilysu ar gyfer gwasanaethau cwmwl ddefnyddio dull dilysu aml-ffactor bob amser
- defnyddio cyfrifon ar wahân i gyflawni gweithgareddau gweinyddol yn unig (dim e-bostio, pori ar y we na gweithgareddau defnyddiwr arferol a allai wneud breintiau gweinyddol yn agored i risgiau y gellid eu hosgoi)
- dileu neu analluogi breintiau mynediad arbennig pan na fydd eu hangen mwyach (pan fydd aelod o staff yn newid rôl, er enghraifft)

Dilysu heb gyfrinair

Dull o gadarnhau pwy yw'r defnyddiwr heb ddefnyddio cyfrineiriau traddodiadol yw dilysu heb gyfrinair.

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Mae enghreifftiau cyffredin o ddulliau dilysu heb gyfrinair yn cynnwys:

- **Pasallweddi:** Technoleg mewngofnodi heb gyfrinair sy'n seiliedig ar gryptograffeg allweddi cyhoeddus a ddefnyddir i ddilysu defnyddiwr yn ddiogel. Mae hyn yn cynnwys dilyswyr FIDO2 sy'n cael eu hystyried yn Basallweddi. Ystyrir bod dilyswyr FIDO2 yn fath o ddilysu aml-ffactor am fod proses dilysu defnyddiwr yn cael ei chyflawni. Mae FIDO2 yn set o safonau sy'n diffinio dilysu cryptograffig gan ddefnyddio manylion a phrotocolau mewngofnodi allweddi cyhoeddus i ddarparu dewisiadau amgen mwy diogel yn lle cyfrineiriau ar gyfer cael mynediad at wasanaethau ar-lein.
- **Dilysu biometrig**: Mae'n defnyddio nodweddion biolegol y defnyddiwr megis olion bysedd neu bryd a gwedd ei wyneb i gadarnhau pwy ydyw
- **Allweddi neu docynnau diogelwch**: Dyfeisiau caledwedd ffisegol megis allweddi diogelwch USB neu gardiau clyfar
- **Hysbysiadau gwthio**: Neges ar ffôn clyfar i gymeradwyo neu wrthod ymgais mewngofnodi
- **Codau untro**: Anfonir codau dros dro drwy e-bost, SMS neu ap symudol

Mae hyn yn helpu i osgoi llawer o'r problemau sy'n gysylltiedig â chyfrineiriau traddodiadol y gellir eu hanghofio, eu dwyn neu eu cael drwy ymosodiad grymus.

Dull dilysu aml-ffactor

Yn ogystal â darparu haen ychwanegol o ddiogelwch ar gyfer cyfrineiriau nad ydynt yn cael eu diogelu gan y rheolaethau technegol eraill, dylech bob amser ddefnyddio dull dilysu aml-ffactor er mwyn amddiffyn cyfrifon gweinyddol a chyfrifon sy'n hygyrch o'r rhyngrwyd ymhellach.

Rhaid i elfen gyfrinair y dull dilysu aml-ffactor fod yn 8 nod o hyd o leiaf, heb gyfyngiad ar yr hyd mwyaf.

Mae pedwar math o ffactor ychwanegol i'w hystyried:

- dyfais a reolir/sefydliad
- ap ar ddyfais ddibynadwy
- tocyn ffisegol ar wahân

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

- cyfrif hysbys neu ddibynadwy

Dylid dewis ffactorau ychwanegol fel eu bod yn hygyrch a bod modd eu defnyddio. Efallai y bydd angen i chi ymgymryd â phrofion defnyddwyr er mwyn penderfynu beth sydd orau i'ch defnyddwyr. I gael rhagor o wybodaeth, gweler canllawiau'r Ganolfan Seiberddiogelwch Genedlaethol ar ddilysu aml-ffactor.

Gwybodaeth: Nid SMS yw'r math mwyaf diogel o ddull dilysu aml-ffactor, ond mae'n cynnig cryn fantais dros beidio â defnyddio dull dilysu aml-ffactor o gwbl. Mae unrhyw ddull dilysu aml-ffactor yn well na pheidio â chael un o gwbl. Fodd bynnag, os oes dulliau amgen ar gael a fydd yn gweithio i'ch sefyllfa, argymhellwn eich bod yn defnyddio'r rhain yn lle SMS.

Dilysu drwy gyfrinair

Mae'n ofynnol i'r defnyddiwr ddilysu ar gyfer pob cyfrif defnyddiwr.

Pan gaiff defnyddwyr eu dilysu gan ddefnyddio cyfrinair, dylech roi'r mesurau amddiffynnol canlynol ar waith:

- Caiff cyfrineiriau eu hamddiffyn rhag cael eu dyfalu drwy rym drwy roi o leiaf un o'r canlynol ar waith:
    - proses ddilysu aml-ffactor (gweler uchod)
    - cyfyngu ar nifer yr ymgeisiau, fel bod yr amser y mae'n rhaid i'r defnyddiwr aros rhwng ymgeisiau yn cynyddu gyda phob ymgais aflwyddiannus. Ni ddylech ganiatáu mwy na 10 cynnig mewn 5 munud
    - cloi dyfeisiau ar ôl dim mwy na 10 ymgais aflwyddiannus
- Defnyddiwch reolaethau technolegol i reoli ansawdd cyfrineiriau. Bydd hyn yn cynnwys un o'r canlynol:
    - Defnyddio dull dilysu aml-ffactor (gweler uchod)
    - Sicrhau bod cyfrineiriau yn 12 nod o leiaf, heb gyfyngiad ar yr hyd mwyaf
    - Sicrhau bod cyfrineiriau yn 8 nod o leiaf, heb gyfyngiad ar yr hyd mwyaf ac atal cyfrineiriau cyffredin yn awtomatig gan ddefnyddio rhestr gwrthod
- Helpu defnyddwyr i ddewis cyfrineiriau unigryw ar gyfer eu cyfrifon gwaith drwy:

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

- addysgu pobl i osgoi defnyddio cyfrineiriau cyffredin, megis enw anifail anwes, patrymau cyffredin ar y bysellfwrdd neu gyfrineiriau y maent wedi'u defnyddio yn rhywle arall. Gallai hyn gynnwys addysgu pobl i ddefnyddio'r nodwedd cynhyrchu cyfrinair sydd wedi'i mewnosod ar rai cyfleusterau rheoli cyfrinair
- annog pobl i ddewis cyfrineiriau hirach drwy hyrwyddo'r defnydd o sawl gair (o leiaf tri) i greu cyfrinair (megis canllawiau'r Ganolfan Seiberddiogelwch Genedlaethol ar ddefnyddio tri gair a ddewisir ar hap)
- darparu man storio diogel ar gyfer cyfrineiriau (er enghraifft, cyfleuster rheoli cyfrineiriau neu gwpwrdd diogel dan glo) gyda gwybodaeth glir am sut a phryd y gellir ei ddefnyddio
- peidio â gorfodi mesurau sy'n golygu bod cyfrineiriau yn dod i ben
- peidio â gorfodi gofynion o ran cymhlethdod cyfrineiriau

Dylech hefyd sicrhau bod proses sefydledig ar waith i newid cyfrineiriau yn brydlon os byddwch yn gwybod neu'n amau bod cyfrinair neu gyfrif dan fygythiad

5. Amddiffyn rhag maleiswedd

Yn gymwys i: Gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, IaaS, PaaS, SaaS

Nod

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Atal maleiswedd hysbys a meddalwedd annibynadwy rhag gweithredu, achosi difrod neu gael gafael ar ddata.

Cyflwyniad

Meddalwedd sy'n cael ei hysgrifennu a'i dosbarthu'n fwriadol i gyflawni gweithredoedd maleisus yw maleiswedd, megis feirysau cyfrifiadurol, mwydod a meddalwedd wystlo. Mae ffynonellau posibl yn cynnwys: atodiadau maleisus ar negeseuon e-bost, lawrlwythiadau (gan gynnwys rhai o siopau cymwysiadau), a gosod meddalwedd anawdurdodedig yn uniongyrchol.

Os caiff system ei 'heintio', mae'n debyg y bydd eich sefydliad yn dioddef problemau megis systemau yn gwrthod gweithio, colli data, neu haint parhaus a fydd yn anweledig nes y bydd yn achosi niwed yn rhywle arall.

Gallwch osgoi'r posibilrwydd o niwed i raddau helaeth drwy:

- atal maleiswedd rhag cael ei chyflwyno i ddyfeisiau
- atal maleiswedd rhag rhedeg ar ddyfeisiau

Enghraifft: Mae Acme Corporation yn defnyddio proses llofnodi digidol ochr yn ochr â rheol sy'n golygu mai dim ond cymwysiadau wedi'u fetio o siop gymwysiadau'r ddyfais all weithredu ar y ddyfais. Ni fydd cymwysiadau anghymeradwy a heb eu llofnodi yn rhedeg ar ddyfeisiau. Mae'r ffaith mai dim ond cymwysiadau dibynadwy (sydd ar y rhestr derbyn) y gall defnyddwyr eu gosod yn golygu bod llai o risg y caiff dyfeisiau eu heintio gan faleiswedd.

Gofynion

Mae'n rhaid i chi sicrhau bod mesur amddiffyn rhag maleiswedd yn weithredol ar bob dyfais o fewn y cwmpas. Ar gyfer pob dyfais, mae'n rhaid i chi ddefnyddio o leiaf un o'r opsiynau a restrir isod. Yn y rhan fwyaf o gynhyrchion modern, bydd yr opsiynau hyn wedi'u cynnwys yn y feddalwedd a ddarperir. Fel arall, gallwch brynu cynhyrchion gan ddarparwr trydydd parti. Ym mhob achos, rhaid i'r feddalwedd fod yn weithredol, cael ei diweddaru yn unol â chyfarwyddiadau'r gwerthwr a'i ffurfweddu i weithio fel y nodir isod:

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Meddalwedd wrthfaleiswedd (opsiwn ar gyfer dyfeisiau o fewn y cwmpas sy'n defnyddio Windows neu MacOS gan gynnwys gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron)

Os byddwch yn defnyddio meddalwedd wrthfaleiswedd i amddiffyn eich dyfais, rhaid ei ffurfweddu fel ei bod yn:

- cael ei diweddaru yn unol ag argymhellion y gwerthwr
- atal maleiswedd rhag rhedeg
- atal cod maleisus rhag cael ei weithredu
- atal cysylltiadau â gwefannau maleisus dros y rhyngrwyd

Rhestr derbyn cymwysiadau (opsiwn ar gyfer pob dyfais o fewn y cwmpas)

Dim ond cymwysiadau cymeradwy, y cyfyngir arnynt drwy broses llofnodi digidol, y caniateir iddynt weithredu ar ddyfeisiau. Mae'n rhaid i chi wneud y canlynol:

- gymeradwyo cymwysiadau o'r fath yn fwriadol cyn eu rhoi ar ddyfeisiau
- cynnal rhestr gyfredol o gymwysiadau cymeradwy, ni ddylai defnyddwyr allu gosod unrhyw gymhwysiad nad yw wedi'i lofnodi neu sydd â llofnod annilys

F. Canllawiau pellach

Dim ymddiriedaeth a Cyber Essentials

Mae saernïaeth rhwydweithiau yn newid. Mae mwy o wasanaethau yn symud i'r cwmwl ac mae'r defnydd o Feddalwedd fel Gwasanaeth (SaaS) yn parhau i gynyddu.

Ar yr un pryd, mae llawer o sefydliadau yn croesawu gweithio hyblyg, sy'n golygu y gall llawer o wahanol fathau o ddyfeisiau gysylltu â'ch systemau o sawl lleoliad. Mae hefyd yn dod yn fwyfwy cyffredin i sefydliadau rannu data â'u partneriaid a defnyddwyr gwadd, sy'n golygu bod angen polisïau rheoli mynediad mwy gronynnog.

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©

Mae saernïaeth dim ymddiriedaeth wedi'i dylunio i ymdopi â'r amodau newidiol hyn drwy alluogi profiad gwell i ddefnyddwyr ar gyfer mynediad o bell a rhannu data.

Dull o ddylunio system yw saernïaeth dim ymddiriedaeth lle caiff ymddiriedaeth hanfodol yn y rhwydwaith ei dileu. Yn hytrach, tybir bod y rhwydwaith yn elyniaethus a chaiff pob cais am fynediad ei ddilysu, yn seiliedig ar bolisi mynediad. Ceir hyder mewn cais drwy adeiladu cyd-destun, sy'n dibynnu ar ddilysu cryf, awdurdodi, iechyd y ddyfais, a gwerth y data a gyrchir.

Wrth i sefydliadau symud tuag at fodelau saernïaeth dim ymddiriedaeth, rydym wedi'i ystyried yn y cyd-destun hwn ac yn hyderus nad yw rhoi'r rheolaethau technegol ar waith yn eich atal rhag defnyddio saernïaeth dim ymddiriedaeth fel y'i diffinnir gan ganllawiau'r Ganolfan Seiberddiogelwch Genedlaethol.

Mae'r holl ddeunydd yn destun Hawlfraint y Goron ©